International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Study of Using Biometric Mechanism in Mobile Banking Application

R.Sundar , M.Ganesan

Abstract—the next generation of banking application won't be on desktop or mainframes but on thesmall devices we carry every day.Secured e-banking on the mobile is the latest issue for all mobileusers.In this paper authors have focused on how biometric mechanism provides the highest securityto the mobile payment.The present security issues surround the loss of personal information throughthe theft of the cell phone.The problems associated with the implementation of a secure e-payment systems in the country stem from card thefts, internet fraud and identity theft etc., which runs into millions of US dollars annually. This has adversely affected the integrity, development of e-commerce and the country's active participation in the international market.The main research focuson the feature extraction from the runtime fingerprint image onthe Android mobile and send to the server for authentication. Anewly proposed Fuzzy Logic Based fingerprint matchingwill be implemented at the server side.

1 INTRODUCTION

The online banking transaction are part of daily routine for an individual.The existing online banking system has several drawbacks.Firstlyhacking,from the internet any one can hack the username and password and the result is third person get access to owner account.As anyone is not with twenty four hours on the internet,i.e.access bank website,it takes some time to know that your account get hacked and third one can get transferthe money to his own account.Secondly, every time one has to carry laptop or PC with you.So for this issue secured payment applications on mobile device.i.e., M-commerce is proposed.

Today is the era of mobile,everyone having the mobile in hands,instead of using the laptop or PC,mobile is the best option to use for the banking purpose.The next generation of banking application won't be on desktops or mainframes but on the small mobile devices we carry every day.Mobile banking mobile location based services,mobile purchasing and so on.This represents an incredible opportunity to enable mobile devices,and universal devices for mobile commerce applications.

2 METHODOLOGY

The online banking transaction are part of daily routine for an individual.The existing online banking system has several drawbacks.Firstlyhacking,from the internet any one can hack the username and password and the result is third person get access to owner account.As anyone is not with twenty four hours on the internet,i.e.access bank website,it takes some time to know that your account get hacked and third one can get transferthe money to his own account.Secondly, every time one has to carry laptop or PC with you.So for this issue secured payment applications on mobile device.i.e., M-commerce is proposed. Today is the era of mobile,everyone having the mobile in hands,instead of using the laptop or PC,mobile

- [1]*R.Sundar, II Year MCA, Priyadarshini Engineering College, Vaniyambadi, Email: ssundar627@gmail.com*
- [2]*M.Ganesan, .professor of MCA, Department of computer Application, Priyadarshini Engineering College, Vaniyambadi, Email:ganesme11@gmail.com*

Existing smart phones in market is a programmable software framework is vulnerable to typical smart phone attacks. Such attack can make the phone partially or fully unusable and cause unwanted SMS/MMS billing.To avoid the general device attack,authors have used the android mobile for the payment application.Android has software stack basedon the Linux kernel and it contain the Android Native Libraries.It also includes the Image processing library that can be used for the processing input images. PDA's and cell phones these days come with fingerprint scanners for authentication and transactions.There are various methods to take the runtime fingerprint.Android is having the inbuilt fingerprint scanner.It is also possible to install the fingerprint in runtime.Even if biometric mobile is not available,the camera with high mega pixel can take the picture and can be processed further for the secured banking in android based mobile device.Here mobile digital camera is used to capture the fingerprint image.Fingerprint is a powerful mechanism in biometric authentication.So here the payment application is secured in all the ways.

is the best option to use for the banking purpose.The next generation of banking application won't be on desktops or mainframes but on the small mobile devices we carry every day.Mobile banking mobile location based services,mobile purchasing and so on.This represents an incredible opportunity to enable mobile devices,and universal devices for mobile commerce applications.

Existing smart phones in market is a programmable software framework is vulnerable to typical smart phone attacks. Such attack can make the phone partially or fully unusable and cause unwanted SMS/MMS billing.To avoid the general device attack,authors have used the android mobile for the payment application.Android has software stack basedon the Linux kernel and it contain the Android Native Libraries.It also includes the Imageprocessing library that can be used for the processing input images. PDA's and cell phones these days come with fingerprint scanners for authentication and transactions.There are various methods to take the runtime fingerprint.Android is having the inbuilt fingerprint scanner.It is also possible to install the fingerprint in runtime.Even if biometric

mobile is not available,the camera with high mega pixel can take the picture and can be processed further for the secured banking in android based mobile device.Here mobile digital camera is used to capture the fingerprint image.Fingerprint is a powerful mechanism in biometric authentication.So here the payment application is secured in all the ways.

2.1 Biometric Authentication

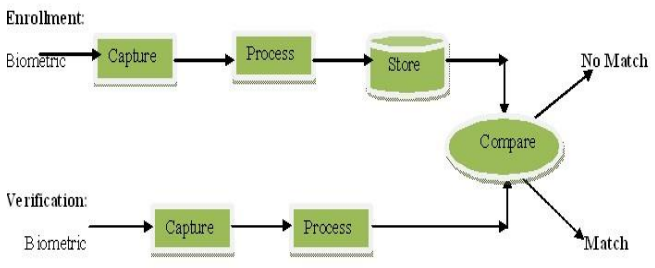
Since biometrics operation is very common application for identification. Worldwide many have worked in the similar area. Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such as your handwritten signature), or something that is a two (such as your voice) [6]. Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use [6],[8]. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode.

2.2 Verification mode

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity [9].

2.3 Identification mode

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an Identity.



2.4 Fingerprints

In order to be used for recognizing a person, the humantrait needs to be unique and not subject to change. Fingerprints, for example, have been used for over one hundred years and, therefore, are generally well accepted as a recognition technology. Other technologies such as face, hand geometry, speaker and iris recognition are also generally accepted. Fingerprints are important. This biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips. These patterns are considered unique to a specific individual. The same fingers of identical t wins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A typical enrollment identifier may include 2 finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints [6], [8]. Since the proposed designed application does not have mobile with scanner, a digital image captured through its 3 pixel camera is being processed for authentication of an individual. Here 3 mega pixel mobile digital cameras are to be used to capture fingerprint images. Images captured with digital camera are distortion free since these images are free from the pressure of contact. Furthermore those images are free from the problems in terms of hygienic, maintenance, latent fingerprint problem and so forth. There are some challenging problems when developing a fingerprint recognition system thatuses the digital camera. The contrast between the ridges and the valleys in fingerprint images obtained with the digital camera, the depth of the field of the camera is small thus some part of the fingerprint regions are in focus but some parts are out of focus, and lastly motion blur in the image acquired[10].

2.5 Feature Extraction

A generic fingerprint authentication system consists of two parts: enrolment and verification. In enrolment, the collected raw fingerprint image is preprocessed, and the features are extracted and stored. In verification the similarity between the enrolled fingerprint features and the features computed from the input fingerprint is examined. Preprocessing is an important stepprior to fingerprint feature extraction. The generic process of preprocessing encompasses segmentation, enhancement, and core point detection. Here the captured fingerprint image is in RG B format is first converted to gray scale. This gray scale image is input to the normalization process. Finger print segmentation is necessary to eliminate the undesired background and re duce the size of the input data. As this is the image captured by digital camera it is difficult to find the minutiae, so contour technique is used to find the region of interest, and then apply the Core point detection method. Usually mobiles are having the digital camera, so to secure the mobile

payment by using bio metric mechanisms captured by digital camera will be more efficient.

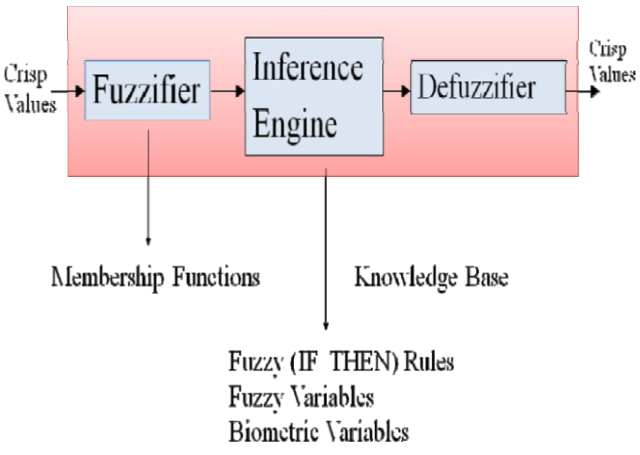
2.6 Secured Transaction

Here authors prefer Android mobile for secure payment application. Themobile phone landscape changed last year with the introduction of smart phones running Android, a platform marketed by Google. Android phones are the first credible threat to the iPhone market. Not only did Google target the same consumers as iPhone, it also aimed to win the hearts and minds of mobile application developers. On the basis of market share and the number of available apps, Android is a success.

Android is an application execution environment for mobile devices. It includes an operating system, application framework, and core applications. The Android software stack is built on the *Linux kernel*, which is used for its device drivers, memory management, process management, and networking. The next level up contains the *Android native libraries*. Various system components in the upper layers use these libraries, which are written in C/C++. Incorporating these libraries in Android applications is achieved via Java Native interfaces. William Enck and his colleagues discussed the main components of an Android application and how to use an Android-specific mechanism to protect Android applications. In general, several security mechanisms are incorporated into the Android framework. We can cluster them into three general groups: Linux mechanisms, environmental features, and Android specific mechanisms.

3 FUZZY LOGIC

Fuzzy logic is a form of many-valued logic, it deals with reasoning that is approximate rather than fixed and exact.



A fuzzy logic controller consists of three main operations: Fuzzification, Inference Engine and Defuzzification. The input sensory (crisp or biometric) data are fed into fuzzy logic rule based system where physical quantities are represented into biometric variables with appropriate membership functions.

These biometric variables are then used in the antecedents (IFPart) of a set of fuzzy "IF-THEN" rules within an inference engine to result in a new set of fuzzy biometric variables or consequent (THEN-Part). Fuzzy logic controller will be design at the server side, Server database contain the extracted features, and controller efficiently match the features of runtime image with the server database.

4 CONCLUSION

The design approach for a biometric mechanism for enchanted security of online transaction on android system has been proposed.Here run time fingerprint would be captured for mobile transaction.Authentication request and reply are in the encrypted form. This gives the better level of security mechanism for mobile payment system. The proposed system can be used in mobile banking and M-commerce.

REFERENCES

[1] Han-Na You,Jae-SikLee,Jung-Jae Kim,Moon-SeogJun,"A study on the two-channel authentication method which providestwo-way authentication in the Internet banking environment"

[2] ChetanaHegde,Manu S,P DeepaShenoy,Venugopal K R,L MPatnaik(2008)"Secure Authentication using Image Processing and Visual Cryptograhy for Banking Applications".

[3] Chang-Burm Cho, A. Chande, Yue Li, and Tao Li, "Workload characterization of biometric applications on Pentium 4 microarchitecture," Workload Communications and Information Characterization Symposium, 2005. Technologies, 2006. ISCIT '06. Proceedings of the IEEE International, International Symposium on, 2006, pp.

[4] "Fingerprints (FPC)-Sensors.", http://www.fingerprints.com / Technology / Sensors.aspx? sc_lang= en.